

CLAIMS

What is claimed is:

1. A system for supervising usage of software comprising:
 - a software vendor producing instances of software;
 - 5 a tag server producing a plurality of tags, one tag per instance of software, each tag uniquely identifying an instance of software with which it is associated;
 - a user device receiving and installing an instance of software and securely receiving a tag uniquely associated with that instance of software, the
 - 10 user device including a supervising program which detects attempts to use the instance of software and which verifies the authenticity of the tag associated with the instance of software before allowing use of the instance of software; and
 - an untagged instance of software used on the user device;
 - 15 wherein the supervising program detects the use of the untagged instance of software and performs a fingerprinting process on the untagged instance of software and stores fingerprints resulting from the fingerprinting process on the user device.
2. The system of claim 1, wherein the user device's supervising program further
- 20 performs a fingerprinting process on a tagged instance of software used on the device and stores the fingerprints resulting from the fingerprinting process in a fingerprint table on the user device.

3. The system of claim 2, wherein the supervising program stores locations from which the fingerprints are computed.
4. The system of claim 2, wherein the fingerprints are based on contents of the instance of software.
- 5 5. The system of claim 2, wherein the fingerprints are based on known sequences of behavior of the instance of software.
6. A user device comprising:
 - an input port receiving an instance of software and receiving a tag uniquely associated with that instance of software and receiving a request to use the instance of software;
 - 10 a processor executing a supervising program, the supervising program detecting the request to use the instance of software and verifying the authenticity of the tag associated with the instance of software before allowing use of the instance of software by the user device; and
 - 15 an untagged instance of software used on the user device;
 - wherein the supervising program detects the untagged instance of software and performs a fingerprinting process on the untagged instance of software and stores fingerprints resulting from the fingerprinting process in a fingerprint table on the user device.
- 20 7. The user device of claim 6, wherein the supervising program determines that a call-up procedure is required as defined by a call-up policy and the supervising program performs the call-up procedure to update the usage status of untagged instances of software stored on the user device.

8. The user device of claim 7, wherein during performing the call-up procedure, the supervising program transmits a portion of the fingerprint table from the user device via an interconnection mechanism coupled to the user device and awaits reception of a continuation message returned to the user device that indicates actions to be performed for each untagged instance of software stored on the user device.
- 5
9. A system for supervising usage of software comprising:
- a software vendor producing instances of software,
 - a user device receiving and installing an instance of software,
 - 10 the user device including a supervising program,
 - an untagged instance of software used on the user device;
 - wherein the supervising program detects the use of the untagged instance of software and performs a fingerprinting process on the untagged instance of software and stores fingerprints resulting from the fingerprinting process on the user device.
- 15
10. The system of claim 9, wherein the user device's supervising program further performs a fingerprinting process on an untagged instance of software used on the device and stores the fingerprints resulting from the fingerprinting process in a fingerprint table on the user device.
- 20
11. The system of claim 10, wherein the supervising program stores locations from which the fingerprints are computed.
12. The system of claim 10, wherein the fingerprints are based on the contents of the instance of software.

13. The system of claim 10, wherein the fingerprints are based on known sequences of behavior of the instance of software.
14. The system of claim 10, further comprising:
a guardian center including:
5 a fingerprint data structure; and
a verification program;
the guardian center periodically communicating with the user device via a call-up procedure to receive all fingerprints from the user device for an instance of software used on the user device, the verification program comparing every
10 fingerprint received from the user device against the fingerprint data structure to determine if an instance of software used on the user device is an infringing instance of software.
15. The system of claim 14, wherein if the verification program detects more than a specified number of matches between fingerprints in the guardian center's
15 fingerprint data structure and fingerprints received from the user device, the verification program specifies a punitive action to be performed, and the verification program returns a continuation message to the user device, the continuation message indicating the punitive action to be performed on the user device.
- 20 16. The system of claim 15, wherein the fingerprint matching process is at least one of general location or same location fingerprint matching.
17. The system of claim 15, wherein the fingerprint matching uses an inverted guardian center fingerprint table.

-111-

18. The system of claim 15, wherein the punitive action specifies that the user device be disabled for a specified length of time.
19. The system of claim 15, wherein the punitive action specifies that the instance of software associated with the fingerprint that was matched to a fingerprint in the fingerprint data structure of the guardian center should be disabled for a specified length of time.
5
20. The system of claim 15, wherein the punitive action depends on at least one of a combination of the history of the behavior of the user device, the history of the behavior of a particular user on the user device, and the collection of other software on the user device.
10
21. The system of claim 14, wherein the software vendor transmits a copy of an infringing instance of software to the guardian center and the guardian center computes fingerprints on the copy of the infringing instance of software and incorporates and stores the fingerprints into the fingerprint data structure on the guardian center.
15